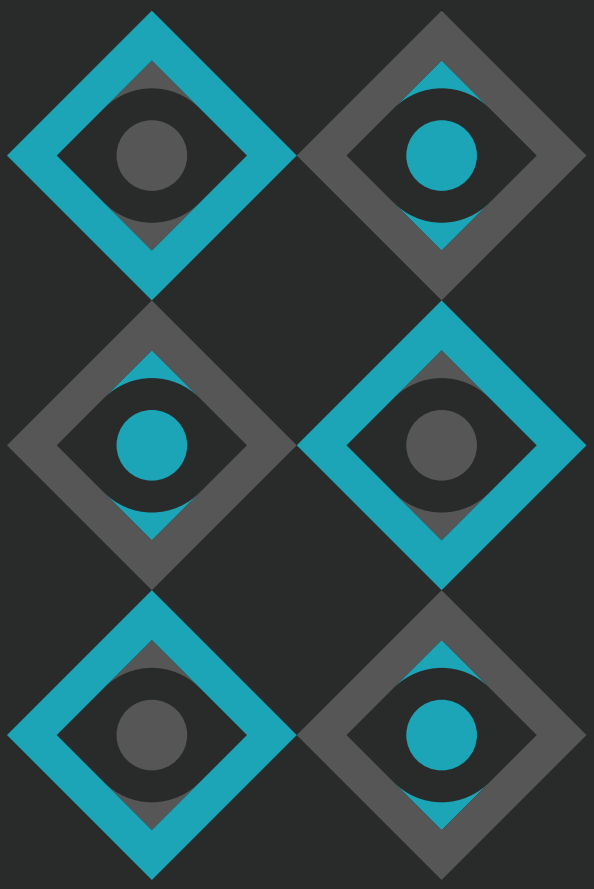
Internet Security Threat Report

Synthèse



Section

01

Symantec™

En 2016, les auteurs de cyberattaques ont affiché de nouvelles ambitions. Cette année a en effet été marquée par des attaques hors normes : hold-up virtuels de plusieurs millions de dollars, tentatives évidentes de déstabilisation du processus électoral aux États-Unis par des groupes soutenus par d'autres puissances, et attaques de déni de service distribué (DDoS) d'une ampleur exceptionnelle, lancées via un réseau de bots constitué d'appareils de l'Internet des objets (IoT).

Si ces cyberattaques ont atteint un niveau de nuisance sans précédent, leurs auteurs se sont souvent contentés d'outils et techniques très simples. Les vulnérabilités Zero Day et les malwares sophistiqués sont désormais utilisés avec parcimonie et les attaquants agissent de moins en moins clandestinement. Ils recourent à des techniques directes, comme le spear-phishing, et exploitent « les ressources disponibles », en utilisant par exemple des logiciels d'administration réseau légitimes ou les fonctions des systèmes d'exploitation.

Mirai, le réseau de bots qui a servi à mener des attaques DDoS majeures, était principalement composé de routeurs et de caméras de sécurité infectés, appareils à faible puissance ou mal sécurisés. Placés entre de mauvaises mains, même les équipements et logiciels les plus inoffensifs peuvent avoir des effets dévastateurs.

Attaques ciblées : subversion et sabotage sur le devant de la scène

Le milieu du cyberespionnage a notablement évolué vers des activités plus manifestes, conçues pour déstabiliser et perturber des entreprises ou des pays spécifiques. Aux États-Unis, les cyberattaques menées contre le Parti démocrate et les fuites d'informations volées qui ont suivi ont été l'un des grands thèmes de l'élection présidentielle. Dans la sphère du renseignement américain, ces attaques, attribuées à la Russie, sont apparemment considérées comme un succès. Il est dès lors probable que ces mêmes tactiques soient réutilisées contre d'autres pays pour influencer la vie politique et semer la discorde.

Les cyberattaques axées sur le sabotage sont traditionnellement rares, mais l'année 2016 a été marquée par deux vagues d'attaques portées par des malwares destructeurs. Un malware permettant d'effacer des disques a été utilisé contre des cibles ukrainiennes au mois de janvier, puis à nouveau en décembre. Ces attaques ont également provoqué des coupures de courant. De son côté, le cheval de Troie Shamoon est réapparu, après quatre ans d'absence, dans des attaques visant plusieurs entreprises saoudiennes.

La recrudescence des attaques de déstabilisation a coïncidé avec le déclin de certaines activités clandestines, en particulier l'espionnage économique et les vols ciblant la propriété intellectuelle et les secrets industriels. À la suite d'un accord conclu en 2015 par les États-Unis et la Chine, par lequel les deux pays renonçaient à l'espionnage économique dans le cyberespace, les détections de malware liées à des groupes chinois soupçonnés d'espionnage ont considérablement chuté. Cela ne signifie pas pour autant que l'espionnage économique a disparu ; ce phénomène est concomitant à l'augmentation d'autres formes d'attaques ciblées, comme les attaques activistes ou financières de haut vol.

Attaques contre les banques : des cibles toujours plus ambitieuses

Jusque récemment, les cybercriminels se concentraient surtout sur les clients des banques, en pillant leurs comptes ou en volant leurs informations de cartes bancaires. Mais désormais, des attaquants d'un nouveau genre, plus ambitieux, s'en prennent directement aux banques, tentant parfois de dérober des millions de dollars en une seule attaque. Des groupes tels que Carbanak ont ouvert la voie et mis en évidence le potentiel d'une telle approche en menant une série d'attaques contre des banques américaines.

Au cours de l'année 2016, deux autres groupes ont relevé la barre en lançant des attaques encore plus ambitieuses. Le groupe Banswift a réussi à dérober 81 millions USD à la banque centrale du Bangladesh en exploitant les faiblesses de la sécurité de l'établissement pour infiltrer son réseau et dérober ses informations d'authentification SWIFT afin de réaliser des opérations frauduleuses.

Une enquête a également montré qu'un autre groupe, connu sous le nom d'Odinaff, montait des attaques sophistiquées contre des banques et autres institutions financières. Apparemment, le groupe utilisait un malware pour dissimuler sur les relevés des clients les messages SWIFT correspondant aux opérations frauduleuses dont il était à l'origine.

Banswift et Odinaff ont fait preuve d'une certaine expertise technique et employé des tactiques généralement réservées aux groupes avancés. Mais certains groupes moins sophistiqués ont également volé des sommes d'argent considérables. Les fraudes BEC, ou fraudes au président, qui s'appuient sur des messages de spear-phishing composés avec beaucoup plus de soin, continuent à faire des ravages : près de 3 millions USD ont été ainsi volés au cours des trois dernières années.

Exploiter les ressources disponibles

Cybercriminels ou groupes soutenus par des États, les attaquants commencent à modifier leurs tactiques : pour piéger leurs victimes, ils utilisent davantage les fonctions des systèmes d'exploitation, des outils en vente libre et des services cloud. Le cas le plus médiatisé est une attaque perpétrée au cours de la campagne électorale américaine. Un simple message de spear-phishing a donné accès au compte Gmail du directeur de campagne d'Hillary Clinton, John Podesta, sans recourir à aucun malware ni aucune vulnérabilité.

Cette tactique, qui consiste à exploiter les ressources disponibles plutôt qu'un malware ou un exploit, offre de nombreux avantages pour les attaquants. Identifier et exploiter des vulnérabilités Zero Day devient plus difficile à mesure que le développement sécurisé et le « bug bounty » se renforcent. Les kits d'attaques web sont moins prisés, sans doute en raison des efforts à fournir pour préserver la fraîcheur des exploits et entretenir une infrastructure back-end.

Les outils de script puissants, comme PowerShell et les macros, sont des fonctions par défaut de Windows et Microsoft Office qui peuvent favoriser l'accès à distance et les téléchargements de malware sans utiliser de vulnérabilités ni d'outils malveillants. Bien qu'elles existent depuis près de 20 ans, les macros Office refont surface dans le paysage des menaces depuis que les attaquants recourent au social engineering afin de contourner facilement les mesures de sécurité mises en place autrefois pour traiter le problème des virus macro.

Si la mise en œuvre est réussie, l'exploitation des outils disponibles peut aboutir à des infections asymptomatiques. Les attaquants n'ont plus besoin d'agir clandestinement.

Résurgence de l'email comme vecteur d'attaque privilégié

Les emails malveillants ont été l'arme de choix de nombreuses cyberattaques en 2016, aussi bien pour les groupes de cyberespionnage soutenus par des États que pour les gangs pratiquant le ransomware de masse. Un email sur 131 envoyés était malveillant, soit le taux le plus élevé depuis 5 ans.

La popularité retrouvée de l'email découle de plusieurs facteurs. C'est un vecteur d'attaque éprouvé. Il ne repose pas sur des vulnérabilités, mais s'appuie sur la simple supercherie pour inciter les victimes à ouvrir une pièce jointe, cliquer sur un lien ou donner des informations d'authentification. Les emails de spear-phishing, comme les faux messages invitant à réinitialiser un mot de passe Gmail, ont été utilisés lors des attaques liées à la campagne électorale américaine.

Dans le même temps, les messages malveillants maquillés en échanges électroniques courants, comme des confirmations de livraison ou des factures, étaient le vecteur de propagation favori des ransomwares. L'existence de réseaux de bots disponibles à la location, comme Necurs, a permis aux groupes de ransomware de mettre sur pied de gigantesques campagnes d'emails au cours de l'année 2016, avec envois quotidiens de centaines de milliers de messages malveillants.

Ransomware : les victimes pressées de payer des montants toujours plus élevés

Le ransomware reste un fléau pour les entreprises et le grand public, avec des campagnes systématiques envoyant des quantités phénoménales d'emails malveillants. Dans certains cas, les entreprises peuvent être dépassées par le volume de messages reçus. Les attaquants exigent de plus en plus de leurs victimes : le montant moyen des rançons était de 1 077 USD en 2016, contre 294 USD l'année précédente.

Les attaquants ont mis au point un modèle économique qui consiste à dissimuler des malwares au sein de messages inoffensifs, à appliquer un chiffrement inviolable sur l'appareil de la victime, puis à réclamer anonymement le paiement d'une rançon en cryptodevises. Face à l'efficacité de ce modèle, ils sont de plus en plus nombreux à prendre le train en marche. Le nombre de nouvelles familles de ransomware découvertes en 2016 a plus que triplé, pour s'établir à 101, et Symantec a enregistré une hausse de 36 % des infections de ce type.

De nouveaux horizons : IoT et cloud dans le collimateur des pirates

Si le ransomware et les fraudes bancaires restent les principales menaces pour les utilisateurs finaux, d'autres dangers commencent à poindre. L'essor des attaques ciblant les appareils IoT n'était qu'une question de temps. L'année 2016 a été marquée par le premier incident majeur avec l'émergence de Mirai, un réseau de bots notamment constitué de routeurs et de caméras de sécurité. La faible sécurité de ces appareils en a fait une cible de choix pour les attaquants, qui ont bâti un réseau de bots suffisamment vaste pour lancer une attaque DDoS sans précédent. Symantec a constaté un doublement des tentatives d'attaques contre les appareils IoT sur l'ensemble de l'année 2016. En période de pic, ces équipements faisaient l'objet d'une attaque toutes les deux minutes en moyenne.

Mirai a ciblé plusieurs services liés au cloud, tel que Dyn, fournisseur de services DNS. Cette attaque, ainsi que le piratage de millions de bases de données MongoDB hébergées dans le cloud, montre bien que les attaques cloud sont désormais une réalité, et elles devraient augmenter en 2017. Le recours de plus en plus fréquent aux services cloud doit devenir un sujet prioritaire au sein des entreprises, car ces services créent un angle mort en termes de sécurité. Symantec a constaté que les entreprises utilisent 928 applications cloud en moyenne, contre 841 plus tôt dans l'année. Comme la plupart des DSI estiment que leur entreprise n'utilise que 30 ou 40 applications cloud, il est donc probable qu'ils sous-estiment le risque et s'exposent à de nouveaux types d'attaques.